

REMARKS

Claims 1, 2, 5-18, 20-30, 32-39 remain in this application. Claims 1, 4, 8-10, 14-16, 18, 20, 24, 30, 32, 36, and 39 have been amended. Claims 1, 15, and 24 are amended to recite “calculating a second hash from the uniform resource locator of the originator in the tag; and authenticating the originator of the packet upon determining the decrypted hash and the second hash are identical.” These features are supported at least on page 15, line 25 to page 16, line 15 of the current specification. Claims 4, 8-10, 14-16, 18, 20, 24, 30, 32, 36, and 39 are amended to be consistent with claims 15 and 24. Claims 3, 4, 19, and 31 are cancelled. Reconsideration of this application in light of the above amendments and the following remarks is requested.

Rejections Under 35 U.S.C. §103(a), Claims 1, 3-5, 8, 11-18, 20, 23, 24, 28-30, and 36-39

Claims 1, 3-5, 8, 11-18, 20, 23, 24, 28-30, and 36-39 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hughes (U.S. Patent No. 6,122,372) in view of Blott (EP 1,054,529A2). Neither Hughes nor Blott discloses “calculating a second hash from the uniform resource locator of the originator in the tag,” as recited in amended claims 1, 15, and 24.

As the PTO recognizes in MPEP § 2142:

... The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness...

It is submitted that, in the present case, the examiner has not factually supported a prima facie case of obviousness for the following, mutually exclusive, reasons.

Even When Combined, the References Do Not Teach the Claimed Subject Matter

The Hughes and Blott references cannot be applied to reject claims 1, 15, and 24 under 35 U.S.C. § 103 which provides that:

A patent may not be obtained ... if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time

the invention was made to a person having ordinary skill in the art to which the subject matter pertains ... (Emphasis added)

Thus, when evaluating a claim for determining obviousness, all limitations of the claim must be evaluated. However, neither Hughes nor Blott discloses “calculating a second hash from the uniform resource locator of the originator in the tag,” as is claimed in claims 1, 15, and 24.

In the rejection of claim 3, the examiner alleges that Hughes discloses these features at column 6, lines 36-53 and column 11, lines 1-25, which read as follows:

FIG. 3 is a system diagram illustrating a system for creating a CNS ID and comparing it to a CNS ID that is encapsulated with a message set that is received. Input data 302 is either received by a party or retrieved from storage by that party. A claimed CNS ID 304 that is claimed to identify input data 302 is also received by the party as part of a message. The party may desire to verify that the claimed CNS ID matches input data 302. To accomplish this, input data 302 is input to a cryptographic hash function 306. The output of cryptographic hash function 306 is a derived CNS ID 308 which is now known by the party to be the proper CNS ID for input data 302. Both derived CNS ID 308 and claimed CNS ID 304 are input to a comparator 310. The output of comparator 312 is a logical indicator of whether or not the input data matches the claimed CNS ID. Thus, the CNS ID is verifiable because it is a data generated ID. Given input data and a specific cryptographic hash function, the CNS ID for the input data may be derived.

In some embodiments a sender tag 214 is provided. Sender tag 214 includes a sender ID that identifies the sender as well as a sender authentication attribute. In certain embodiments, the sender ID and sender authentication may be combined or authentication may be omitted if, for example, the network being used is secure and the presence of the sender on the network is sufficient to authenticate the sender. Benefits are realized, however from providing the sender ID separately from authentication. In a preferred embodiment, the authentication is provided by the sender signing a hash of a portion of the encapsulated message with his private key. In one embodiment, the portion of the message that is hashed and signed by the sender is message portion 220. Finally, the close tag 216 indicates the end of the encapsulated message.

As noted above, self tag 201 includes a CNS message ID. The CNS message ID is a cryptographic hash of the message set, which includes the tags shown in FIG. 2 as message portion 220. Thus, the message set that is hashed includes the sender ID and the close tag. Therefore, when the receiver confirms a message by and identifies the message with the message ID, the receiver is not only confirming receipt of the message body and message interpretation ID's, but is also confirming receipt of the user ID and user authentication.

In the first section, Hughes merely discloses creating a CNS ID by inputting input data into a cryptographic hash function to generate a derived CNS ID. **However, Hughes does not disclose or suggest that the input data used to calculate a hash is from a uniform resource locator of the originator in the tag. In fact, there is no mention of a uniform resource locator of the originator in the input data.** At column 6, lines 22-25, Hughes merely discloses that "the data to be identified, whether it be a message, template, protocol, contract or some other form of document, is used as input to the cryptographic hash function." Therefore, Hughes does not disclose "calculating a second hash from the uniform resource locator of the originator in the tag" of claims 1, 15, and 24.

In the second section, Hughes merely discloses a self tag that includes a CNS message ID, which is a hash of a message set. *There is no mention that the tag includes a uniform resource locator of the originator from which a second hash is calculated.* While Hughes discloses that the message set that is hashed includes the sender ID, the sender ID is not part of the tag. To the contrary, the sender ID is part of the hash. This is different from the presently claimed disclosure in that the sender ID of Hughes is included in the encrypted hash instead of the tag. In addition, there is no mention of the sender ID being a uniform resource locator of the originator. Therefore, Hughes does not disclose or suggest the features of claims 1, 15, and 24.

The examiner further states that while Hughes does not disclose the identifier of the originator is an address, Blott discloses these features in paragraphs 36-39. Applicant respectfully disagrees. In paragraph 39, Blott discloses using a source IP address field and the source port field of the received data packet to associate a service with the received data packet. However, there is no disclosure or suggestion that the source IP address is used to calculate a hash. Therefore, Blott also does not disclose the features of claims 1, 15, and 24.

The examiner further alleges that it would be obvious to one of ordinary skill in the art to incorporate network usage billing system of Blott into the encapsulated message authentication system of Hughes in order to allow the system to monitor and modify a user's quality of service so as to provide appropriate billing for such usage depending on the level of quality of service the user receives and wishes to receive. Applicant respectfully disagrees.

Instead of calculating a second hash from a uniform resource locator of the originator in the tag, Hughes calculates a CNS ID from input data without mention of a uniform resource locator of the originator. In addition, Hughes specifically includes a sender ID in the hash instead of the tag. Blott, on the other hand, merely discloses associating a service from a source IP address field of a received data packet. There is no mention of calculating a hash from the source IP address field of the data packet. Therefore, one of ordinary skill would not have been led to modify or combine the disclosures of Hughes and Blott to reach the features of claims 1, 15, and 24.

Accordingly, Applicant respectfully requests the withdrawal of rejection to claims 1, 3-5, 8, 11-18, 20, 23, 24, 28-30, and 36-39 under 35 U.S.C. § 103(a).

Application No. 10/035,653
Reply to Office Action of March 2, 2006

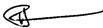
Docket No.: 14686RRUS01U (22171.386)
Customer No. 27683

Conclusion

It is clear from all of the foregoing that independent claims 1, 15, and 24 are in condition for allowance. Dependent claims 1, 2, 5-14, 16-18, 20-23, 25-30, 32-39 depend from and further limit independent claims 1, 15, and 24 and therefore are allowable as well.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,



Wing Y Mok
Registration No. 56,237

Dated: August 1, 2006

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972/739-8626
Facsimile: 972/692-9075
Client Matter No.: 14686RRUS01U
(22171.386)

R-142159.1

Certificate of Service

I hereby certify that this correspondence is being filed with the U.S. Patent and Trademark Office via EFS-Web on August 1, 2006.


Linda Ingram